

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri**FILED**MAY 11 2021U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUISIn the Matter of the Search of
THE PREMISES LOCATED AT: 6218 Virginia Avenue,
St. Louis, MO, 63111, within the Eastern District of
Missouri. SEE ATTACHMENT A) 4:21 MJ 5129 NAB
) **FILED UNDER SEAL**
) SIGNED AND SUBMITTED TO THE COURT FOR
) FILING BY RELIABLE ELECTRONIC MEANS
)
)**APPLICATION FOR A SEARCH WARRANT**I, David Rapp, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:**See Attachment A**located in the Eastern District of Missouri, there is now concealed**See Attachment B**

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- xx evidence of a crime;
 xx contraband, fruits of crime, or other items illegally possessed;
 xx property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

Title Section

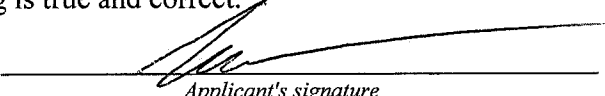
Title 18, United States Code, Sections 2251(a) and 2252A (production and trafficking of child pornography 0

The application is based on these facts:


SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.


 Applicant's signature
 David Rapp, SA, FBI
 Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 05/11/2021

 Judge's signature
City and State: St. Louis, MO
 Honorable Nannette A. Baker, U.S. Magistrate Judge
 Printed name and title

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT: 6218) No. 4:21 MJ 5129 NAB
Virginia Avenue, St. Louis, MO, 63111,)
within the Eastern District of Missouri.) **FILED UNDER SEAL**
SEE ATTACHMENT A) SIGNED AND SUBMITTED TO THE COURT FOR
) FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David Rapp, a Special Agent with the Federal Bureau of Investigation, being duly sworn,
depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (“SA”) of the FBI since March of 2001 and am currently assigned to the St. Louis Division. While employed by the FBI, I have investigated federal criminal violations related to technology or cybercrime, child exploitation, and child pornography. I have gained experience through training provided by the FBI and through everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. During my time as a case agent on numerous complex investigations, I utilized a variety of investigative techniques to include organizing and participating in physical surveillance; participating in undercover operations; serving search warrants; making arrests; and interviews involving defendants. Moreover, I am a federal law

enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the premises located at 6218 Virginia Avenue, St. Louis, MO, 63111 (the “SUBJECT PREMISES”), the content of computers, wireless telephones, electronic storage devices, storage media, digital cameras, and DEVICES located therein, and the person of **Kevin Matthew WATTS** if he is located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252, and 2252A, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251(a) and 2251(e)

(production and attempted production of child pornography). are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

d. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, having a minor assist any other person to engage in, or transporting any minor in or affecting interstate or foreign commerce, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if completed or attempted in or affecting interstate or foreign commerce, by any means, including by computer, or utilizing materials that had been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. “Bulletin Board” means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video

images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as “internet forums” or “message boards.” A “post” or “posting” is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message “thread,” often labeled a “topic,” refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through “private messages.” Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. “Chat room,” as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. “Child pornography,” as defined in 18 U.S.C. § 2256(8), includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, or the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. “Cloud storage,” as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user’s computer or other local storage device) and is made available to users over a network, typically the Internet.

g. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such

as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i. “Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone” as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

j. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that

creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

k. As used herein, the term “DEVICES,” refers to computer, storage medium, computer hardware, digital media storage, digital cameras, digital video recorders, or cell phones.

l. The “Domain Name System” or “DNS” is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

m. “Encryption” is the process of converting data into a code in order to prevent unauthorized access to the data.

n. A “hidden service,” also known as an “onion service,” is website or other web service that is accessible only to users operating within the Tor anonymity network.

o. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

p. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

q. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

r. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

s. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

t. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

u. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

v. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

w. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

x. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

y. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

z. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

aa. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

PROBABLE CAUSE

6. On May 3, 2021, writer contacted an individual whose initials are A.G. in reference to her 17-year-old daughter whose initials are C.F. A.G. advised that she had recently discovered that her daughter, C.F., had been involved in a sexual relationship with Kevin WATTS, a 35-year-old man. WATTS was also C.F.'s manager at the Qdoba restaurant that she worked at located at the South County Mall. A.G. advised that she also believed C.F. and WATTS had exchanged sexually explicit images with each other as she had observed some of these images on C.F.'s Apple iPhone.

7. A.G. advised that she discovered the relationship after conducting a "find my iPhone" search on CF's Apple iPhone on approximately March 30, 2021. The results took A.G. to the intersection of Virginia and Iron in St. Louis, MO. A.G. waited at the intersection and eventually saw C.F. and WATTS exit 6218 Virginia Avenue, St. Louis, MO. A.G. recorded WATTS' vehicle's Missouri license plate at that time as ND2V5H.

8. On May 6, 2021, writer interviewed C.F. in reference to her relationship with WATTS and the potential that child sexual abuse material (CSAM) had been created and shared via text messages. C.F. admitted to your affiant that she was involved in a sexual relationship with WATTS and that she also traded sexually explicit images with WATTS.

9. C.F. advised that she had initially met WATTS when she started working at Qdoba in September of 2020. C.F. advised that sometime around March, 2021, WATTS became a "line manager" and at that point C..F provided him with her phone number for scheduling purposes. Shortly after giving WATTS her phone number, C.F. stated that WATTS began texting her inappropriate, sexual in nature messages. WATTS also started calling C.F. on her Apple iPhone

at that time as well. C.F. knew WATTS to have a newer model Apple iPhone and also that he drove a silver in color Chevrolet passenger vehicle.

10. C.F. advised that she “brushed off” WATTS inappropriate texts and calls, but approximately one week after having C.F.’s telephone number, WATTS asked her to come over to his residence, 6218 Virginia Avenue, St. Louis, MO. C.F. went over to WATTS’ residence and at that time a sexual relationship began between the two. C.F. believed she and WATTS had sexual intercourse approximately 5 times between that day and April 5, 2021.

11. C.F. advised that during this time frame, she and WATTS exchanged numerous nude images of themselves via text message. C.F. advised that the images she took of herself were still on her Apple iPhone, but that she deleted all the text messages she had with WATTS after her mother discovered her relationship with him. All of the nude images that WATTS sent C.F. were attached in the text messages that C.F. had deleted and CF did not download the images directly to her phone. C.F. believed that she sent images to WATTS sometime around the third week of March, 2021.

12. A forensics exam conducted by the FBI on C.F.’s Apple iPhone identified multiple images that constitute CSAM. C.F. advised that these were the images that she texted and shared with WATTS, after WATTS asked her to send naked photos of her to him. C.F. advised that she sent WATTS naked photos of herself on two separate occasions. C.F. advised that WATTS sent her a picture of his penis on two separate occasions as well in return for her photos. There was a specific image taken from C.F.’s Apple iPhone which shows C.F. and a white, male lying in a bed, in which the white, male is not wearing a shirt and displaying a “Darth Vader” tattoo on his chest. C.F. confirmed that this was an image of her and WATTS and that this image was taken on one of

the occasions that she was at WATTS' residence. C.F. advised WATTS had multiple tattoos, including the aforementioned Darth Vader tattoo and another one that depicted a "dragon".

13. An additional photograph was forensically located on C.F.'s Apple iPhone which depicted a white, erect penis. C.F. advised that this was one of the photos that Watt had sent her and that she had believed that she had deleted this photo from her phone. C.F. believed the photo to be of WATTS' penis.

14. Law enforcement Database checks confirmed WATTS' address to be 6218 Virginia Avenue, St. Louis, MO, while also providing his date of birth (DOB) to be 02/xx/1986, and Social Security Number (SSN) to be a number ending in 6839. A Department of Motor Vehicle check confirmed WATTS' address, SSN and DOB, while also describing him as being 5'11", 155 pounds, with the middle name "Matthew" and being the registered owner of a 2014 Chevrolet Sedan, with Missouri license plate ND2V5H. An employment check with the State of Missouri advised that WATTS was employed by the Qdoba Restaurant Corporation for the time period July, 2019 through March, 2021, which was the last quarter that employment history had been reported by the State. The employment check also listed his mailing address as 6218 Virginia Avenue, St. Louis, MO.

15. On the afternoon of May 7, 2021, your affiant drove to 6218 Virginia Avenue, St. Louis, MO to do a spot check on the residence. At that time, your affiant observed a silver, Chevrolet Cruze, Missouri license plate ND2V5H parked on Virginia Avenue in front of the 6218 Virginia Avenue. Your affiant also observed two males on the front porch of 6218 Virginia Avenue, one of which your affiant positively identified as WATTS.

16. On the morning of May 10, 2021, your affiant conducted another spot check of 6218 Virginia Avenue, St. Louis, MO. At that time your affiant observed the same Chevrolet Cruze with Missouri license plate ND2V5H parked at the intersection of Iron Street and Virginia Avenue, in very close proximity to the 6218 Virginia Avenue address.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

17. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic

communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of

software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT
TO VIEW CHILD PORNOGRAPHY**

18. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged

in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic

tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).

19. Based on all of the information contained herein, I believe that WATTS, residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access child sexual abuse and exploitation material and utilize computer devices and telephones to store child sexual abuse and exploitation material. For example, the target of investigation obtained photographs consisting of child sexual abuse material from an underage juvenile relative to this investigation, according to the victim.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

20. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. I submit that if a computer, storage medium, or DEVICE is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer, storage medium, or DEVICE, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

22. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers and DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the

computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location

of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

23. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers and DEVICES, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not

always possible to search computer equipment, DEVICES, and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching DEVICES and computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can

easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

24. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator’s network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals

who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

25. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

26. This warrant permits law enforcement to compel WATTS to unlock any computer, computer storage, computer hardware, or cell phone (hereinafter, “DEVICES”) owned or used by WATTS requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera

detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the

device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES owned or used by WATTS that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of WATTS to the fingerprint scanner of the DEVICES owned or used by WATTS found at the SUBJECT PREMISES; (2) hold the DEVICES owned or used by WATTS found at the SUBJECT PREMISES in front of the face of WATTS and activate the facial recognition feature; and/or (3) hold the DEVICES owned or used by WATTS found at the SUBJECT PREMISES in front of the face of WATTS and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize nor prohibit law enforcement from requesting that WATTS provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize nor prohibit law enforcement from asking WATTS to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

27. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.


28. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

[THE REMAINDER OF THIS PAGE LEFT INTENTIONALLY BLANK]

REQUEST FOR SEALING

29. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

I state under the penalty of perjury that the foregoing is true and correct.



DAVID RAPP
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on the 11 day of May, 2021.



HONORABLE NANNETTE A. BAKER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The location to be searched (the “SUBJECT PREMISES”) is known as 6218 Virginia Avenue, St. Louis, MO, 63111, and includes the residential building, any outbuildings, any vehicles in the garage and/or driveway, and any appurtenances thereto, and is described as a white in color, two story residence with the numbers 6218 displayed to the left of the front door, with a large purple flag hanging from a patio bannister and with a large white refrigerator on the front porch..



Front photo of 6218 Virginia taken on 5.10.2021



Side photo of 6218 Virginia taken on 5.10.21



Subject vehicle parked in front of 6218 Virginia taken the afternoon of 5.7.21



Subject vehicle parked on Iron Road at intersection of Virginia taken in the morning on 5.10.21

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

All records, items, and information constituting evidence, instrumentalities and contraband concerning the violations of Title 18, United States Code, Sections 2251(a) and 2252A (production and trafficking of child pornography), including as follows:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:

a. any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);

b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and

c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession or production of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents and records regarding the ownership and/or possession of the SUBJECT PREMISES.

6. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.

7. During the execution of the search of the Premises described in Attachment A, law enforcement personnel are also specifically authorized to obtain from persons located on the SUBJECT PREMISES at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Devices requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the Device(s) found at the SUBJECT PREMISES for which law

enforcement can reasonably identify the user of the Device(s) without the use of biometrics;

b. where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant; for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

8. The proposed warrant does not authorize (nor does it prohibit) law enforcement to request that the aforementioned person(s) state or otherwise provide the password or any other means that may be used to unlock or access the Device(s). Moreover, the proposed warrant does not authorize (nor does it prohibit) law enforcement to ask the aforementioned person(s) to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s).